

بحث مختصر في **API**

Registry Functions

For Visual Basic

أعداد المبرمج :مشتاق طالب رشيد العامري

Mushtaq_talib58@yahoo.com

2009

شركة الأميرال للخدات البرمجية المتطورة



Registry Functions

For Visual Basic

الدوال المستخدمة :

RegCloseKey RegConnectRegistry
RegCreateKey RegCreateKeyEx
RegDeleteKey RegDeleteValue
RegEnumValue RegEnumKey
RegEnumKeyEx RegFlushKey
RegGetKeySecurity RegLoadKey
RegNotifyChangKeyValue RegOpenKey
RegQueryInfoKey RegQueryMultipleValues
RegQueryValues RegQueryValueEx
RegReplaceKey RegRestoreKey
RegSaveKey RegSetKeySecurity
RegSetValue RegSetValueEx
RegUnloadKey

السجلات المستخدمة:

SECURITY_ATTRIBUTES FILETIME
SECURITY_DESCRIPTOR ACL

الثوابت المستخدمة:

HKEY_CLASSES_ROOT HKEY_CURRENT_CONFIG
HKEY_CURRENT_USER HKEY_DYN_DATA
HKEY_LOCAL_MACHINE HKEY_PERFORMANCE_DATA
HKEY_USERS ERROR_SUCCESS
ERROR_INSUFFICIENT_BUFFER MAX_PATH
READ_CONTROL KEY_SET_VALUE
KEY_QUERY_VALUE KEY_CREATE_SUB_KEY
KEY_CREATE_LINK KEY_ENUMERATE_SUB_KEYS
KEY_EVENT KEY_NOTIFY
SYNCHRONIZE STANDARD_RIGHTS_ALL
STANDARD_RIGHTS_WRITE STANDARD_RIGHTS_READ
KEY_READ KEY_WRITE

3

KEY_ALL_ACCESS REG_BINARY
REG_CREATED_NEW_KEY REG_DWORD

REG_DWORD_BIG_ENDIAN REG_DWORD_LITTLE_ENDIAN REG_EXPAND_SZ REG_NOTIFY_CHANGE_NAME REG_LINK REG_MULTI_SZ REG_NONE REG_NOTIFY_CHANGE_LAST_SET REG_NOTIFY_CHANGE_SECURITY REG_OPENED_EXISTING_KEY REG_OPTION_BACKUP_RESTORE REG_OPTION_CREATE_LINK REG_OPTION_NON_VOLATILE REG_OPTION_RESERVED REG_OPTION_VOLATILE REG_REFRESH_HIVE REG_RESOURCE_LIST REG_SZ REG_WHOLE_HIVE_VOLATILE REG_LEGAL_CHANGE_FILTER REG_LEGAL_OPTION REG_FULL_RESOURCE_DESCRIPTOR REG_NOTIFY_CHANGE_ATTRIBUTES REG_RESOURCE_REQUIREMENTS_LIST

4

التمهيد:

تتكون ال Registry طبعاً من Keys و Values.

أما ال Keys:

فهي تحتوي على SubKeys وهي عبارة عن Keys وتحتوي على Values

و بفتح ال Registry باستخدام البرنامج regedit.exe تظهر لنا ال keys في الناحية اليسرى من الشاشة و ال Values في الناحية اليمنى.

وهذه صورة توضح ذلك:

5

يمكن إنشاء أو تغيير ال keys وال Values يدوياً بسهولة ولكن كيف يمكن فعل كل ذلك بلغة Visual Basic؟

قبل البدء يجب معرفة بعض الأساسيات للتعامل مع ال Registry.

1. يجب فتح ال Key المراد وضع أو تغيير ال values الموجودة بداخله

2. تغيير القيم الموجودة داخله.

3. إغلاق ال Key الذي تم فتحه. وهذه النقطة مهمة جداً لأنه من دوا لا يتم كتابة البيانات في ال Registry.

ملاحظة: يمكن كتابة البيانات في ال Registry بدون إغلاق ال Key وذلك باستعمال الدالة RegFlushKey ولكن هذه الدالة تستخدم مصادر النظام بشكل كبير حيث يراعى استخدامها إلا في حالات الضرورة القصوى.

شرح النقاط السابقة:

1. فتح ال key.

يجب قبل فتح key معرفة handle ل key آخر يجب أن يكون مفتوح مسبقاً ويجب أن يكون ال key المراد فتحه عبارة عن subkey ل key الذي يوجد لدينا ال handle الخاص به.

تتسآءل الآن كيف يمكنني معرف ال handle الخاص بال key __________ الأب؟

إجابة هذا السؤال عندي ولله الحمد وهي بسيطة.

يعطي نظام التشغيل Windows أرقام ثابتة للمفاتيح الرئيسية كلما تم تشغيل النظام وهذه ال keys مع ال handles الخاصة ا:

Const HKEY_CLASSES_ROOT =&H80000000
Const HKEY_CURRENT_USER =&H80000001
Const HKEY_LOCAL_MACHINE =&H80000002
Const HKEY_USERS =&H80000003
Const HKEY_CURRENT_CONFIG =&H80000005
Const HKEY_DYN_DATA =&H80000006
Const HKEY_PERFORMANCE_DATA =&H80000004

وهذه صورة توضح السابق:

6

وتسمى ال keys السابقة ب predefined keys

والدوال المستخدمة لفتح ال keys هي :

RegOpenKey, RegOpenKeyEx
RegCreateKey,RegCreateKeyEx

. كتابة وحذف البيانات:2

يمكن استخدام الدوال التالية:

RegSetValueEx, RegSetValue) وذلك لتخصيص بيانات Data ل (key معين.

RegSetValue تتعامل مع النصوص فقط، وسأتي شرحها في حينها. :

RegSetValueEx يمكنها كتابة أي نوع من البيانات وهذه الدالة بإمكاا إنشاء : key و value خاص به في نفس الوقت!!!

ولحذف Value من key تستخدم الدالة RegDeleteValue

ولحذف key نستخدم الدالة RegDeleteKey مع ملاحظة أن ال key المحذوف لايتم إزالته حتى يتم قفل آخر handle له.

7ولتغيير أمان ال keys نستخدم RegSetKeySecurity

يمكن جلب ال subkeys ل key معين حتى يتم إيجاد key معين وأخذ البيانات منه : وذلك باستخدام الدالة RegEnumKey أو الدالة RegEnumKeyEx أما الأولى ترجع ال subkeys فقط والثانية ترجع ال subkeys مع ال Classes

لإرجاع بيانات مفصلة حول subkey معينة، البرنامج يمكن أن تستدعي الدالة RegQueryInfoKey

والدالة RegGetKeySecurity ترجع نسخة من ال SecurityDescription التي تحمي ال key

ولجلب ال valuesو ال keyتستخدم الدالة RegEnumValue
. إغلاق ال3 keyيتم باستخدام الدالة RegCloseKey

كل ماعليك فهمه من النقاط السابقة (إن لم تفهم شيئاً منه) هو التالي:

يجب فتح ال keyثم تغير فعل ماتريد عليه ثم بعد ذلك إغلاقه .

01يوجد برنامج في الد المسمى Exampفيه بعض الدوال السابقة.

لقد قمت بشرح عام على بعض الدوال وإليك بشرح مفصل.

8

الباب الأول: التعامل مع ال Keys

الدالة الأولى RegCloseKey :

هي دالة تقوم بإزالة الحجز عن keyتم فتحه وتعريفها ذا الشكل:

تستقبل هذه الدالة معامل واحد فقط وهو:

hKeyهو ال : handleل key تم فتحه

إذا نجحت هذه الدالة فإا سترجع القيمة ERROR_SUCCESS
أما إذا أخفقت فإا ترجع قيمة غير الصفر. , 0والتي تساوي

مع ملاحظة أنه لايمكن استعمال ال handleالذي تم قفله إلا إذا تم
فتح ال keyمن جديد مع ملاحظة أن ال handle سيتغير.

وعليك أن لاتترك ال keyمفتوح أكثر من الوقت الذي تستعمله فيه.

مع ملاحظة أنه لا يتم تخزين البيانات التي تم إضافتها إلى ال Registry
فعلياً إلا عندما يتم قفل ال Key.

وعند كتابة بيانات كبيرة جداً في ال Registryوتنفيذ هذه الدالة قد
10تأخذ بضع ثواني في تخزين البيانات في ال Registry.

الدالة الثانية RegCreateKey :

هذه الدالة تقوم بإنشاء keyمحدد أما إذا كان موجوداً فإا تقوم بفتحه.

هذه الدالة متوافقة مع نظام Windows. 32أما البرامج المعتمدة على win فمن الأفضل
3.1
إستخدام الدالة RegCreateKeyExوالتي سأقوم بشرحها بعد هذه الدالة.

هذه الدالة تقوم باستقبال ثلاث معاملات hKey, lpSubKey,phkResult :

hKeyمن نوع : Long

يشير إلى handleل keyمفتوح حالياً، أو أي من ال Predefinedkeys
(راجع الفصل الثاني لمعرفة ماهي ال PredefinedKeys)

وال keyالمنشأ هو subkeyل keyالمعرف بواسطة hKey.

lpSubKeyمن نوع : String

يحدد إسم ال Keyالمراد إنشاءه أو فتحه وهذا ال Keyيجب أن يكون مفتاح
فرعي من ال Keyالمحدد في hKey.

ويمكن أن يكون إسم واحد أو مسار ذا الشكل:

"SOFTWARE"

أو

"\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"

phkResultمن نوع : **Long**

يؤشر إلى متغير يستقبل ال **Handle**الخاص بال **Key**التي تم فتحها.

القيمة المرجعة:

ترجع هذه الدالة القيمة **ERROR_SUCCESS**إذا نجحت.

ملاحظة:

يمكن إنشاء مجموعة من ال **Keys**المتداخلة.

02ومثال على ذلك يوجد في الد المسمى **Examp**

11

: الدالة الثالثة **RegCreateKeyEx**

هذه الدالة تشبه الدالة السابقة من حيث أا تقوم بإنشاء **Key**أو تفتحه إن كان موجوداً

وتستقبل هذه الدالة تسع معاملات :

hKey, lpSubKey, vReserved, lpClass, dwOption, samDesired, lpSecurityAttributes, phkResult, lpdwDisposition

hKeyمن النوع : **Long**

قيمة ال **Handle**لمفتاح مفتوح حالياً (راجع الدالة السابقة)

lpSubKeyمن النوع : **String**

يشير إلى متغير نصي يحمل اسم ال **subkey**الذي يجب أن يكون متفرع من المفتاح المشار إليه ب **hKey**.

" وهذا المعامل لا يمكن أن يكون\مع ملاحظة أن النص يجب أن لا يبدأ ب "

فارغاً.

Reservedمن النوع : **Long**

هذا المعامل محجوز ويجب أن يكون صفر.

lpClassمن النوع : **String**

متغير نصي يحوي نوع ال **Object**لهذا ال **key**

أما إذا كان ال **key**موجود فإن هذا المعامل يتجاهل.

لن أشرح ال **Classes**الآن لما يحتاجه من وقت وجهد.

dwOptionمن نوع : **Long**

ملاحظة: هذه الخاصية موجودة في **Windows NT 2000**و **Windows**

أما في **Windows 9x**نه يتم تجاهلها. ____________فإ

هذا المعامل يحدد خيارات خاصة بال **Key**.

وهذا يجب أن يكون واحداً من القيم التالية:

REG_OPTION_NON_VOLATILE *or* REG_OPTION_VOLATILE
12
REG_OPTION_NON_VOLATILE
المفتاح المنشأ باستخدام هذا الثابت ليس من السهولة ضياع البيانات الموجودة به وهذا هو الخيار الافتراضي. حيث أن المعلومات تخزن في ملف وتحمى أو تحفظ عندما يعاد تشغيل النظام.
REG_OPTION_VOLATILE
ال Keyالمنشأ باستخدام هذا الثابت تخزن في الذاكرة وغير محفوظة حفظ جيد
وهذا الثابت يتم تجاهله إذا كان ال keyموجود.
REG_OPTION_BACKUP_RESTORE
إذا كانت هذا الثابت موجود فإن الدالة تتجاهل المعامل samDesired
وتعطي صلاحية فتح ال keyعلى أساس Restore, Backup
samDesiredمن نوع Long
يبين كيفية أو نوع الأمن المراد استخدامه لل keyالمراد فتحه.
وهذا المعامل يمكن أن يكون مزيجاً من القيم التالية:
يمكنك القيام بأي شيء ممكن KEY_ALL_ACCESS
صلاحية إنشاء ربط رمزي KEY_CREATE_LINK
إمكانية إنشاء مفاتيح فرعية KEY_CREATE_SUB_KEY
صلاحية عد ومعرفة أسماء المفاتيح الفرعية KEY_ENUMERATE_SUB_KEYS
صلاحية قراءة وتنفيذ KEY_EXECUTE
صلاحية الإعلام بالتغيير KEY_NOTIFY
خليط من مجموعة من الصلاحيات KEY_READ
صلاحية تغيير بيانات المفاتيح الفرعية KEY_SET_VALUE
خليط من مجموعة من الصلاحيات KEY_WRITE
lpSecurityAttributes: من نوع التركيبة SECURITY_ATTRIBUTES
13
هذا المعامل يحدد هل ال handleالمرجع يمكن أن يكون موروثاً بواسطة المعالجة الإبن (ولن أفصل هذه النقطة لما يتطلبه من وقت وجهد).
أما إذا كان هذا المعامل NULLفإن ال handleلا يمكن أن يورث لمعالجة إبن.
وسأشرح هذه التركيبة بعد قليل.
تحت نظام التشغيل Windows NT:
العنصر lpSecurityDescriptorفي هذه التركيبة يوضح صفة الأمان للمفتاح الجديد وإن كان NULLفإن الأمن يأخذ ال Defaults
تحت نظام التشغيل Windows 9x:
العنصر lpSecurityDescriptorيتم تجاهله.
phkResultمن النوع : Long

تقوم هذه الدالة بوضع ال handleلل key المفتوح أو المنشأ ليتم إستخدامه من قبل المبرمج.

lpdwDesposition: من النوع : **Long**

تقوم الدالة بوضع إحدى القيم التالية:

REG_CREATED_NEW_KEY
REG_OPENED_EXISTING_KEY

أما الأول فيدل على أن المفتاح ليس موجود وتم إنشاءه، أما الثاني فإنه يدل على أن المفتاح موجود ولكن تم فتحه فقط بدون أي تغيير.

يمكن الاستفادة من هذه القيمة لمعرفة هل هذه هي أول مرة تم فيها فتح البرنامج أم لا؟

القيمة المرجعة من الدالة:

إذا نجحت الدالة فإا ترجع القيمة **ERROR_SUCCESS**

03يوجد مثال على هذه الدالة في الد المسمى **Examp** ولكن يجب أن تدرس التركيبة التالية حتى تتمكن من فهم هذه الدالة جيداً

14

ملاحظة:

عند إنشاء أو فتح ال **Keys** استخدم

RegCreateKeyEx أو **RegOpenKeyEx**

ولاتسخدم

RegCreateKey و **RegOpenKey**

وذلك حتى تتمكن من استخدام بعض الدوال الأخرى.

15

التركيبة **SECURITY_ATTRIBUTES**

تتكون هذه التركيبة من :

nLength من نوع **Long**
lpSecurityDescriptor من نوع **Long**
bInheritHandle من نوع **Long**

العنصر **nLength**:

يوضع به حجم هذه التركيبة بالبايت، ويجب عليك وضع حجم هذه التركيبة في هذا المتغير باستخدام الدالة **Len**.

العنصر **lpSecurityDescriptor**:

يشير إلى صفة الأمان التي يتحكم ا ال **Object** الذي يتحكم بمشاركته.

وإن كان **NULL**) فإن الدالة قد تعين الأمن الأساسي **Default**)

للبرنامج المستدعي للدالة.

العنصر **bInheritHandle** من نوع **Long**

تحدد ما إذا كان ال **Handle** المرجع موروث عند إنشاء المعالجة الجديدة أم لا فإذا كان **TRUE** فإن المعالجة الجديدة تورث ال

.Handle

03راجع المثال الموجود في الد المسمى: Examp

16

: الدالة الرابعة RegDeleteKey

في نظام التشغيل Windows 9xهذه الدالة تمسح ال keyوجميع محتوياته.

أما في Widnows NTفإن هذه الدالة لايمكن أن تمسح ال keyالموجود به مفاتيح فرعية إذ عليك مسح ال keysالداخلية ثم الخارجية.

وتستقبل هذه الدالة معاملان هما:

hKeyمن نوع Longيحوي ال handleلمفتاح مفتوح مسبقاً

lpSubKeyمن نوع Stringاسم المفتاح المراد حذفه.

القيمة المرجعة:

إذا نجحت الدالة فإا ترجع قيمة ERROR_SUCCESS
04وراجع المثال الموجود في الد المسمى Examp
هذه أربعة دوال على إنشاء وفتح وإغلاق ال keys
) ولكن يمكننا أن نضع قيم أي Valuesفي تلك المفاتيح التي تم فتحها أو إنشاءها (

كيف يمكن ذلك ؟ إليك بالتالي.

17

الباب الثاني: التعامل مع ال Values

الدوال التي تتعامل مع ال valuesوالتي سنشرحها هاهنا هي:

1. RegSetValue
2. RegSetValueEx
3. RegDeleteValue

ملاحظات:

تستخدم هذه الدوال بعد فتح ال Keyوقبل إغلاقه لأنك لو أقفلت ال Keyفلن تستطيع التعامل معه إلا إذا تم فتحه مرة أخرى.

: الدالة الخامسة RegSetValue

هذه الدالة تخصص قيمة للمفتاح وهي قيمة يجب أن تكون Stringولايمكن أن تملك
3.1إسم وهذه الدالة متوافقة مع نظام التشغيل Win
Winمن الأفضل أن يستخدموا الدالة RegSetValueExوالتي تسمح لهم بتخصيص
32مبرمجي
أي عدد من القيم الحاملة للأسماء ومن أي نوع ممكن.

وهذه صورة توضح الفرق بين الدالتين:

18

الدالة RegSetValueمعاملات: 5تستقبل

hKeyيحمل ال handle ال keyمفتوح حالياً.

lpSubKeyعنوان المفتاح الفرعي المراد تخزين ال valueبداخله.

وإذا كان هذا المعامل يساوي vbNullStringفإن ال valueتضاف
إلى ال keyالمشار إليه ب hKey.

dwTypeهذا المعامل يجب أن يكون REG_SZ
ولتخزين أنواع أخرى استخدم الدالة RegSetValueEx
lpDataيحتوي على النص المراد تخصيصه ل value
cbDataيحتوي على طول lpData بالبايت مع مراعاة أنه لا يتم حساب حرف
()اية السلسة الحرفية. وتستخدم الدالةLenلمعرفة طول النص.

: القيمة المرجعة: إذا نجحت الدالة فإا ترجع القيمة ERROR_SUCCESS

. إذا كان الد غير موجود فإن هذه الدالة تنشئه.

19. طول الValue 2محدد على حسب الذاكرة.

بايت في 2048. يجب عليك أن لا تخزن البيانات التي هي أطول من 3

ال Regsitrtإذ أن ذلك يقلل من سرعة الجهاز والحل هو أن تقوم
بحفظها في ملفات وتخزن أسماءها في ال Registry.

05والمثال الموجود في الد المسمى Exampيوضح هذه الدالة.

20

: الدالة السادسة RegSetValueEx:

) تخزن بياناتData) في حقل القيمة (Value Field ال (keyمفتوح حالياً، وكذلك

يمكنها تخصيص معلومات إضافية عن ال Values ال keyمحدد.

تستقبل هذه الدالة المعاملات التالية:

hKeyال : handle ال keyمفتوح مسبقاً.

lpValueNameهو عبارة عن نص يحمل اسم القيمة المراد تغييرها وإن لم تكن :

موجودة فإن الدالة تقوم بإنشاءها فإذا كانت هذه القيمة
vbNullStringوكانت قيمة المعامل dwTypeهي REG_SZ
فإن الدالة تقوم بالعمل ك RegSetValue
Reservedهو متغير محجوز ويجب أن يكون صفراً. :

dwTypeيحدد نوع المعلومات التي ستخزن في ال : valueوهذا المعامل

يجب أن يكون واحداً من القيم التالية:

REG_BINARYقيم ثنائية
REG_DWORDبت 32رقم من
REG_DWORD_LITTLE_ENDIANبت 32رقم من
REG_DWORD_BIG_ENDIANبت 32رقم من
REG_EXPAND_SZسلسلة حرفية تحوي على متغيرات
%" تدل على مراجع مثلPATH"%

REG_LINKرابط برموز Unicode

REG_MULTI_SZمصفوفة تحتوي على Stringsمنتهية
بحرفين لإاء السلسلة.

REG_NONEقيمة من نوع غير معروفة
REG_RESOURCE_LISTقائمة لمراجع الأوامر
التي تصدر من الحاسوب إلى الأجهزة الخارجية.

REG_SZسلسلة حرفية وهي تكون من نوع Unicode
أو من نوع Ansiوذلك حسب استعمالك.

lpDataيؤشر لمتغير يحتوي على البيانات التي ستخزن في اسم القيمة المحدد وهو :

يكون من أي نوع حسب ماحددنا له في المعامل dwType.

21

مع ملاحظة هامة جداً : يجب أن يبعت هذا المعامل بالقيمة

) وليس بالمرجع أي باستخدامByVal)lpDataإذ بدون هذه
الطريقة لن تخزن البيانات صحيحة وسنرى أا ستظهر على
شكل Garbageوعند استخدام ByValتظهر البيانات
صحيحة

cbDataطول المعلومات المراد مبعوثة في : lpDataبالبايت وإن كانت البيانات

من نوع REG_SZأو REG_EXPAND_SZأو
REG_MULT_SZيجب أن يحتوي الطول على الحرف المنتهي به
السلسة الحرفية.

القيمة المرجعة:

إذا نجحت فترجع ERROR_SUCCESSو إلا فقيمة غيرها.

ملاحظة: لاتقوم بتخزين الملفات والأيقونات و الملفات التنفيذية في ال

Registryينها في ____________حتى لايتم إنقاص سرعة الجهاز وقم بتخز
ملفات خارج ال Registry.

أما نحن الهاكر فنقوم بتخزين الملفات التنفيذية
الضارة و الفيروسات هناك لصغر حجمها إذ لايتعدى الملف
32كيلو بايت واحد فقط وأنصحكم بالتحول إلى لغة الأسمبلي
بت إذ أنني أستعمل المترجم MASMومحرر النصوص
RadAsmوهي لغة أفضل من ال Visual Basicولكنني لا
أنقص من هذه اللغة إذ أمضيت معها سنوات لا يفتح برنامج في
جهازي إلا هذه اللغة Visual Basicوعملت برامج عديدة
06المثال الموجود في الد المسمى Exampيوضح الدالة RegSetValueEx
22

: الدالة السابعة RegDeleteVaue

تستخدم هذه الدالة لمسح قيمة من ال Registry
وتستقبل المعاملات التالية:

hKeyيحمل : handleال keyمفتوح حالياً.

lpValueNameيحمل اسم ال : Valueالمراد حذفه وإذا كانت vbNullString

فإا تزيل ال قيمة التي تم وضعها باستخدام الدالة
RegSetValue
القيمة المرجعة من الدالة:

ترجع هذه الدالة إذا نجحت القيمة **ERROR_SUCCESS**
07المثال الموجود في الد المسمى **Examp**يوضح الدوال الثلاثة السابقة

<u>تم بحمد الله و نعمته</u>

أعداد المبرمج :مشتاق طالب رشيد العامري

Mushtaq_talib58@yahoo.com

2009

شركة الأميرال للخدات البرمجية المتطورة